3 Inner products and orthogonality: Linear algebra review

3.1 Bilinear forms

Let $\mathbb{F}$ be a field and let V be an $\mathbb{F}$-vector space. A *bilinear form on* V is a function

$$\begin{array}{rccc} \langle,\rangle\colon & V\times V & \to & \mathbb{F} \\ & (v,w) & \longmapsto & \langle v,w\rangle \end{array} \qquad \text{such that}$$

(a) If $v_1, v_2, w \in V$ then $\langle v_1+v_2, w\rangle = \langle v_1, w\rangle + \langle v_2, w\rangle$,

(b) If $v, w_1, w_2 \in V$ then $\langle v, w_1+w_2\rangle = \langle v, w_1\rangle + \langle v, w_2\rangle$,

(c) If $c \in \mathbb{F}$ and $v, w \in V$ then $\langle cv, w\rangle = c\langle v, w\rangle$,

(d) If $c \in \mathbb{F}$ and $v, w \in V$ then $\langle v, cw\rangle = c\langle v, w\rangle$.

A bilinear form $\langle,\rangle\colon V\times V\to\mathbb{F}$ is *symmetric* if it satsfies:

(S) If $v, w \in V$ then $\langle v, w\rangle = \langle w, v\rangle$.

A bilinear form $\langle,\rangle\colon V\times V\to\mathbb{F}$ is *skew-symmetric* if it satsfies:

(A) If $v, w \in V$ then $\langle v, w\rangle = -\langle w, v\rangle$.

3.2 Sesquilinear forms

Let $\mathbb{F}$ be a field and let $\overline{}\colon \mathbb{F}\to\mathbb{F}$ be a function that satisfies:

$$\text{if } c, c_1, c_2 \in \mathbb{F} \text{ then } \quad \overline{c_1+c_2} = \overline{c_1}+\overline{c_2}, \quad \overline{c_1c_2} = \overline{c_2}\,\overline{c_1} \quad \text{and} \quad \overline{1}=1 \quad \text{and} \quad \overline{\overline{c}} = c.$$

The favourite example of such a function is complex conjugation. The other favourite example is the identity map $\mathrm{id}_{\mathbb{F}}$.

Let V be an $\mathbb{F}$-vector space. A *sesquilinear form on* V is a function

$$\begin{array}{rccc} \langle,\rangle\colon & V\times V & \to & \mathbb{F} \\ & (v,w) & \longmapsto & \langle v,w\rangle \end{array} \qquad \text{such that}$$

(a) If $v_1, v_2, w \in V$ then $\langle v_1+v_2, w\rangle = \langle v_1, w\rangle + \langle v_2, w\rangle$,

(b) If $v, w_1, w_2 \in V$ then $\langle v, w_1+w_2\rangle = \langle v, w_1\rangle + \langle v, w_2\rangle$,

(c) If $c \in \mathbb{F}$ and $v, w \in V$ then $\langle cv, w\rangle = c\langle v, w\rangle$,

(d) If $c \in \mathbb{F}$ and $v, w \in V$ then $\langle v, cw\rangle = \overline{c}\langle v, w\rangle$.

A *Hermitian form* is a sesquilinear form $\langle,\rangle\colon V\times V\to\mathbb{F}$ such that

(H) If $v, w \in V$ then $\langle v, w\rangle = \overline{\langle w, v\rangle}$.

3.3 Gram matrix of $\langle,\rangle$ with respect to a basis B

Assume $n \in \mathbb{Z}_{>0}$ and $\dim(V) = n$. Let $\langle,\rangle\colon V\times V\to\mathbb{F}$ be a bilinear form and let $B = \{b_1,\ldots,b_n\}$ be a basis of V. The *Gram matrix of* $\langle,\rangle$ *with respect to the basis* B is

$$G_B \in M_n(\mathbb{F}) \qquad \text{given by} \qquad G_B(i,j) = \langle b_i, b_j\rangle.$$

Let $C = \{c_1, \ldots, c_n\}$ be another basis of V and let P_{CB} be the change of basis matrix given by

$$c_i = \sum_{i=1}^{n} P_{BC}(j,i) b_j, \qquad \text{for } i \in \{1, \ldots, n\}.$$

Since

$$G_C(i,j) = \langle c_i, c_j \rangle = \sum_{k,l=1}^{n} \langle P_{BC}(k,i) b_k, P_{BC}(l,j) b_l \rangle = \sum_{k,l=1}^{n} P_{BC}(k,i) G_B(k,l) P_{BC}(l,j),$$

then

$$G_C = P_{BC}^t G_B P_{BC},$$

3.4 Quadratic forms

Let $\mathbb{F}$ be a field, V an $\mathbb{F}$-vector space and $\langle , \rangle \colon V \times V \to \mathbb{F}$ a bilinear form. The *quadratic form associated to* $\langle , \rangle$ is the function

$$\| \ \|^2 \colon V \to \mathbb{F} \qquad \text{given by} \qquad \|v\|^2 = \langle v, v \rangle.$$

Theorem 3.1. *Let V be a vector space over a field $\mathbb{F}$ and let $\langle , \rangle \colon V \times V \to \mathbb{F}$ be a bilinear form. Let $\| \ \|^2 \colon V \to \mathbb{F}$ be the quadratic form associated to $\langle , \rangle$.*

(a) (Parallelogram property) If $x, y \in V$ then

$$\|x+y\|^2 + \|x-y\|^2 = 2\|x\|^2 + 2\|y\|^2.$$

(b) (Pythagorean theorem) If $x, y \in V$ and $\langle x, y \rangle = 0$ and $\langle y, x \rangle = 0$ then

$$\|x\|^2 + \|y\|^2 = \|x+y\|^2.$$

(c) (Reconstruction) Assume that $\langle , \rangle$ is symmetric and that $2 \neq 0$ in $\mathbb{F}$. Let $x, y \in V$. Then

$$\langle x, y \rangle = \tfrac{1}{2}(\|x+y\|^2 - \|x\|^2 - \|y\|^2).$$

Theorem 3.2. *Let $\mathbb{F}$ be a field with an involution $\overline{\ \ } \colon \mathbb{F} \to \mathbb{F}$ such that the fixed field*

$$\mathbb{K} = \{a \in \mathbb{F} \mid a = \bar{a}\} \qquad \text{is an ordered field.}$$

For $a \in \mathbb{K}$ define

$$|a|^2 = a\bar{a}.$$

Let V be an $\mathbb{K}$-vector space with a sesquilinear form $\langle , \rangle \colon V \times V \to \mathbb{F}$ such that

(a) If $x, y \in V$ then $\langle y, x \rangle = \overline{\langle x, y \rangle}$.

(b) If $x \in V$ then $\langle x, x \rangle \in \mathbb{K}_{\geq 0}$.

Let $\| \ \| \colon V \to \mathbb{F}$ be the corresponding quadratic form and assume that if $a \in \mathbb{K}_{\geq 0}$ then there exists a unique $c \in \mathbb{K}_{\geq 0}$ such that $c^2 = a$. Then

(c) (Cauchy-Schwarz) If $x, y \in V$ then $|\langle x, y \rangle| \leq \|x\| \cdot \|y\|$.

(d) (Triangle inequality) If $x, y \in V$ then $\|x+y\| \leq \|x\| + \|y\|$.

The proof of Theorem 3.16 uses the following proposition.

Proposition 3.3. *Let $\mathbb{F}$ be an ordered field and let $x, y \in \mathbb{F}$ with $x \geq 0$ and $y \geq 0$. Then*

$$x \leq y \qquad \text{if and only if} \qquad x^2 \leq y^2.$$

3.5 Nondegeneracy and dual bases

Let V be a $\mathbb{F}$-vector space with a sesquilinear form $\langle,\rangle\colon V \to \mathbb{F}$. The form $\langle,\rangle$ is *nondegenerate* if it satisfies

$$\text{if } v \in V \text{ and } v \neq 0 \text{ then there exists } w \in V \text{ such that } \langle v, w\rangle \neq 0.$$

An alternative way of stating this condition is to say $V \cap V^\perp = 0$. Another alternative is to say that the map

$$\begin{matrix} V & \to & V^* \\ v & \mapsto & \varphi_v \end{matrix} \qquad \text{given by} \qquad \varphi_v\colon \begin{matrix} V & \to & \mathbb{F} \\ w & \mapsto & \langle v, w\rangle \end{matrix}$$

is an *injective* linear transformation.

Let $k \in \mathbb{Z}_{>0}$ and assume that $W \subseteq V$ is a subspace of V with $\dim(W) = k$. Let $(w_1, \ldots, w_k)$ be a basis of W. A *dual basis to* $(w_1, \ldots, w_k)$ *with respect to* $\langle,\rangle$ is a basis $(w^1, \ldots, w^k)$ of W such that

$$\text{if } i, j \in \{1, \ldots, k\} \text{ then } \quad \langle w^i, w_j\rangle = \delta_{ij}.$$

Proposition 3.4. *Let V be a vector space with a sesquilinear form $\langle,\rangle\colon V \times V \to \mathbb{F}$. Let $W \subseteq V$ be a subspace of V. Assume W is finite dimensional, that $(w_1, \ldots, w_k)$ is a basis of W and that G is the Gram matrix of $\langle,\rangle$ with respect to the basis $\{w_1, \ldots, w_k\}$. The following are equivalent:*

(a) A dual basis to $(w_1, \ldots, w_k)$ exists.

(b) G is invertible.

(c) $W \cap W^\perp = 0$.

(d) The linear transformation

$$\Psi_W\colon \begin{matrix} W & \to & W^* \\ v & \longmapsto & \varphi_v \end{matrix} \qquad \textit{given by} \qquad \varphi_v(w) = \langle v, w\rangle,$$

is an isomorphism.

3.6 Isotropy and nondegeneracy

Let $W \subseteq V$ be a subspace of V. The *orthogonal to W* is

$$W^\perp = \{v \in V \mid \text{if } w \in W \text{ then } \langle v, w\rangle = 0\}.$$

The subspace W is *nonisotropic* if $W \cap W^\perp = 0$.

Proposition 3.5. *A sesquilinear form $\langle,\rangle\colon V \times V \to \mathbb{F}$ satisfies*

(no isotropic vectors condition) If $v \in V$ and $\langle v, v\rangle = 0$ then $v = 0$.

if and only if it satisfies

(no isotropic subspaces condition) If W is a subspace of V then $W \cap W^\perp = 0$.

Remark 3.6. Let $V = \mathbb{C}\text{-span}\{e_1, e_2\}$ with symmetric bilinear form $\langle,\rangle\colon V \times V \to \mathbb{C}$ with Gram matrix

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \qquad \text{in the basis } \{e_1, e_2\}.$$

This form has isotropic vectors since $\langle e_1, e_1\rangle = 0$. The dual basis to $\{e_1, e_2\}$ is the basis $\{e_2, e_1\}$. Letting

$$\begin{aligned} b_1 &= \tfrac{1}{\sqrt{2}}(e_1 + e_2), \\ b_2 &= \tfrac{i}{\sqrt{2}}(e_1 - e_2), \end{aligned} \qquad \text{then the Gram matrix is} \qquad \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

with respect to the basis $\{b_1, b_2\}$ and $b_1 + ib_2$ is an isotropic vector.

3.7 Orthogonal projections

Let $\mathbb{F}$ be a field and let V be an $\mathbb{F}$-vector space. Let $\langle,\rangle\colon V\times V\to\mathbb{F}$ be a sesquilinear form.

Let $k\in\mathbb{Z}_{>0}$ and let W be a subspace of V such that $\dim(W)=k$ and $W\cap W^\perp=0$.

Let $(w_1,\ldots,w_k)$ be a basis of W and let $(w^1,\ldots,w^k)$ be the dual basis of W (which exists by Proposition 3.4). The *orthogonal projection onto* W is the function

$$P_W\colon V\to V \qquad \text{given by} \qquad P_W(v)=\sum_{i=1}^k \langle v,w_i\rangle w^i.$$

The following proposition shows that P_W does not depend on which choice of basis of W is used to construct P_W.

Proposition 3.7. *(Characterization of orthogonal projection) Let $\mathbb{F}$ be a field and let V be an $\mathbb{F}$-vector space. Let $\langle,\rangle\colon V\times V\to\mathbb{F}$ be a sesquilinear form. Let $k\in\mathbb{Z}_{>0}$ and let W be a subspace of V such that $\dim(W)=k$ and $W\cap W^\perp=0$. The orthogonal projection onto W is the unique linear transformation $P\colon V\to V$ such that*

(1) If $v\in V$ then $P(v)\in W$.

(2) If $v\in V$ and $w\in W$ then $\langle v,w\rangle=\langle P(v),w\rangle$.

3.8 Orthogonal projections produce orthogonal decompositions

Let $\mathbb{F}$ be a field and let V be an $\mathbb{F}$-vector space. Let $\langle,\rangle\colon V\times V\to\mathbb{F}$ be a sesquilinear form.

Let $k\in\mathbb{Z}_{>0}$ and let W be a subspace of V such that $\dim(W)=k$ and $W\cap W^\perp=0$.

The following proposition explains how the orthogonal projection onto W produces the decomposition $V=W\oplus W^\perp$.

Theorem 3.8. *Let $n\in\mathbb{Z}_{>0}$ and let V be an inner product space with $\dim(V)=n$. Let W be a subspace of V such that $W\cap W^\perp=0$. Let P_W be the orthogonal projection onto W and let $P_{W^\perp}=1-P_W$. Then*

$$P_W^2=P_W,\quad P_{W^\perp}^2=P_{W^\perp},\quad P_WP_{W^\perp}=P_{W^\perp}P_W=0,\quad 1=P_W+P_{W^\perp},$$
$$\ker(P_W)=W^\perp,\qquad \mathrm{im}(P_W)=W\quad\text{and}\qquad V=W\oplus W^\perp.$$

3.9 Orthonormal sequences and Gram-Schmidt

A *Hermitian form* is a sesquilinear form $\langle,\rangle\colon V\times V\to\mathbb{F}$ such that

(H) If $v,w\in V$ then $\langle v,w\rangle=\overline{\langle w,v\rangle}$.

An *orthonormal sequence* in V is a sequence $(b_1,b_2,\ldots)$ in V such that

$$\text{if } i,j\in\mathbb{Z}_{>0}\quad\text{then}\quad \langle b_i,b_j\rangle=\begin{cases}1, & \text{if } i=j,\\ 0, & \text{if } i\neq j.\end{cases}$$

Proposition 3.9. *Let V be an $\mathbb{F}$-vector space with a Hermitian form. An orthonormal sequence $(a_1,a_2,\ldots)$ in V is linearly independent.*

3.10 Orthonormal bases

Let $n \in \mathbb{Z}_{>0}$ and let V be an inner product space with $\dim(V) = n$. An *orthonormal basis of* V, or *self-dual basis of* V, is a basis $\{u_1, \ldots, u_n\}$ such that

$$\text{if } i, j \in \{1, \ldots, n\} \quad \text{then} \quad \langle u_i, u_j \rangle = \begin{cases} 0, & \text{if } i \neq j, \\ 1, & \text{if } i = j. \end{cases}$$

An *orthogonal basis in* V is a basis $\{b_1, \ldots, b_n\}$ such that

$$\text{if } i, j \in \{1, \ldots, n\} \quad \text{and } i \neq j \quad \text{then} \quad \langle b_i, b_j \rangle = 0.$$

The following theorem guarantees that, in some favourite examples, orthonormal bases exist.

Theorem 3.10. *(Gram-Schmidt) Let V be an $\mathbb{F}$-vector space with a sesquilinear form $\langle , \rangle \colon V \times V \to \mathbb{F}$. Assume that $\langle , \rangle$ is nonisotropic and that $\langle , \rangle$ is Hermitian i.e.,*

(1) (Nonisotropy condition) If $v \in V$ and $\langle v, v \rangle = 0$ then $v = 0$, and

(2) (Hermitian condition) If $v_1, v_2 \in V$ then $\langle v_2, v_1 \rangle = \overline{\langle v_1, v_2 \rangle}$.

Let $p_1, p_2, \ldots$ be a sequence of linear independent elements of V.

(a) Define $b_1 = p_1$ and

$$b_{n+1} = p_{n+1} - \frac{\langle p_{n+1}, b_1 \rangle}{\langle b_1, b_1 \rangle} b_1 - \cdots - \frac{\langle p_{n+1}, b_n \rangle}{\langle b_n, b_n \rangle} b_n, \qquad \textit{for } n \in \mathbb{Z}_{>0}.$$

Then $(b_1, b_2, \ldots)$ is an orthogonal sequence in V.

(b) Assume that $\mathbb{F}$ is a field in which square roots can be made sense of and that if $v \in V$ and $v \neq 0$ then $\langle v, v \rangle \neq 0$. Define

$$\|v\| = \sqrt{\langle v, v \rangle}, \qquad \textit{for } v \in V.$$

Let $(b_1, \ldots, b_n)$ be an orthogonal basis of V. Define

$$u_1 = \frac{b_1}{\|b_1\|}, \quad \ldots, \quad u_n = \frac{b_n}{\|b_n\|}.$$

Then $(u_1, \ldots, u_n)$ is an orthonormal basis of V.

3.11 Adjoints of linear transformations

Let V be an $\mathbb{F}$-vector space with a nondegenerate sesquilinear form $\langle , \rangle \colon V \times V \to \mathbb{F}$. Let $f \colon V \to V$ be a linear transformation.

- The *adjoint of f with respect to* $\langle , \rangle$ is the linear transformation $f^* \colon V \to V$ determined by

$$\text{if } x, y \in V \text{ then} \quad \langle f(x), y \rangle = \langle x, f^*(y) \rangle.$$

- The linear transformation f is *self adjoint* if f satisfies:

$$\text{if } x, y \in V \quad \text{then} \quad \langle f(x), y \rangle = \langle x, f(y) \rangle.$$

- The linear transformation f is an *isometry* if f satisfies:

$$\text{if } x,y\in V \quad \text{then} \quad \langle f(x), f(y)\rangle = \langle x,y\rangle.$$

- The linear transformation f is *normal* if $ff^* = f^*f$.

Let $\{w_1,\ldots,w_k\}$ be a basis of W and assume that the dual basis $\{w^1,\ldots,w^k\}$ of W exists. If $w = c_1w^1 + \cdots c_kw^k$ then $c_j = \langle w, w_j\rangle$ and so

$$w = \langle w, w_1\rangle w^1 + \cdots + \langle w, w_k\rangle w^k.$$

If $w\in W$ then

$$f^*(w) = \langle f^*(w), w_1\rangle w^1 + \cdots + \langle f^*(w), w_k\rangle w^k = \langle w, f(w_1)\rangle w^1 + \cdots + \langle w, f(w_k)\rangle w^k,$$

and this specifies $f^*\colon W\to W$ in terms of f. Then

$$f \text{ is self adjoint if } f = f^* \qquad \text{and} \qquad f \text{ is an isometry if } ff^* = 1,$$

HW: Let $V = \mathbb{F}^n$ with basis $(e_1,\ldots,e_n)$ and inner product given by

$$e_i = \begin{pmatrix} 0\\ \vdots\\ 0\\ 1\\ 0\\ \vdots\\ 0\end{pmatrix} \quad \text{with 1 in the } i\text{th row} \quad \text{and} \quad \langle e_i, e_j\rangle = \delta_{ij}.$$

Let $f\colon V\to V$ be a linear transformation of V and let A be the matrix of f with respect to the basis $(e_1,\ldots,e_n)$. Show that, with respect to the basis $(e_1,\ldots,e_n)$,

$$\text{the matrix of } f^* \text{ is} \qquad A^* = \overline{A}^t.$$

Since

$$\sum_{i=1}^n A^*(i,j)e_i = f^*(e_j) = \sum_{i=1}^n \langle e_j, f(e_i)\rangle e_i = \sum_{i=1}^n\sum_{k=1}^n \langle e_j, A(k,i)e_k\rangle e_i = \sum_{i=1}^n \overline{A(j,i)}e_i,$$

then $A^*(i,j) = \overline{A(j,i)}$.

3.12 The Spectral theorem

Let $A\in M_n(\mathbb{C})$ and let $V=\mathbb{C}^n$ with inner product given by

$$\left\langle \begin{pmatrix} x_1\\ \vdots\\ x_n\end{pmatrix}, \begin{pmatrix} y_1\\ \vdots\\ y_n\end{pmatrix}\right\rangle = x_1\overline{y_1} + \cdots x_n\overline{y_n}. \tag{3.1}$$

Let $A\in M_n(\mathbb{C})$.

- The *adjoint of A* is the matrix $A^* \in M_n(\mathbb{C})$ given by $A^*(i,j) = \overline{A(j,i)}$.
- The matrix A is *self adjoint* if $A = A^*$.
- The matrix A is *unitary* if $AA^* = 1$.
- The matrix A is *normal* if $AA^* = A^*A$.

Write $A^* = \overline{A}^t$. The *unitary group* is

$$U_n(\mathbb{C}) = \{U \in M_n(\mathbb{C}) \mid UU^* = 1\}.$$

Theorem 3.11. *Let $V = \mathbb{C}^n$ with inner product given by (3.1). The function*

$$\begin{matrix} \left\{ \begin{matrix} \text{ordered orthonormal bases} \\ (u_1, \ldots, u_n) \text{ of } \mathbb{C}^n \end{matrix} \right\} & \longrightarrow & U_n(\mathbb{C}) \\ (u_1, \ldots, u_n) & \longmapsto & U = \begin{pmatrix} | & & | \\ u_1 & \cdots & u_n \\ | & & | \end{pmatrix} \end{matrix} \qquad \text{is a bijection.}$$

The following proposition explains the role of normal matrices.

Proposition 3.12. *Let $V = \mathbb{C}^n$ with inner product given by (3.1). Let*

$$A \in M_n(\mathbb{C}), \qquad \lambda \in \mathbb{C} \qquad \text{and} \qquad V_\lambda = \ker(\lambda - A).$$

If $AA^* = A^*A$ then

$$V_\lambda \text{ is } A\text{-invariant}, \quad V_\lambda^\perp \text{ is } A\text{-invariant}, \quad V_\lambda \text{ is } A^*\text{-invariant and} \quad V_\lambda^\perp \text{ is } A^*\text{-invariant}.$$

Theorem 3.13. *(Spectral theorem)*
Let $n \in \mathbb{Z}_{>0}$ and $V = \mathbb{C}^n$ with inner product given by (3.1).

(a) Let $n \in \mathbb{Z}_{>0}$ and $A \in M_n(\mathbb{C})$ such that $AA^* = A^*A$. Then there exists a unitary $U \in M_n(\mathbb{C})$ and $\lambda_1, \ldots, \lambda_n \in \mathbb{C}$ such that

$$U^{-1}AU = \mathrm{diag}(\lambda_1, \ldots, \lambda_n).$$

(b) Let $f : V \to V$ be a linear transformation such that $ff^* = f^*f$. Then there exists an orthonormal basis $(u_1, \ldots, u_n)$ of V consisting of eigenvectors of f.

HW: Show that if $A \in M_n(\mathbb{C})$ is self adjoint then its eigenvalues are real.
HW: Show that if $U \in M_n(\mathbb{C})$ is unitary then its eigenvalues have absolute value 1.

Theorem 3.14. *(Spectral theorem)*
Let $n \in \mathbb{Z}_{>0}$ and $V = \mathbb{C}^n$ with inner product given by (3.1).

(a) Let $n \in \mathbb{Z}_{>0}$ and $A \in M_n(\mathbb{C})$ such that $AA^* = A^*A$. Then there exists a unitary $U \in M_n(\mathbb{C})$ and $\lambda_1, \ldots, \lambda_n \in \mathbb{C}$ such that

$$U^{-1}AU = \mathrm{diag}(\lambda_1, \ldots, \lambda_n).$$

(b) Let $f : V \to V$ be a linear transformation such that $ff^* = f^*f$. Then there exists an orthonormal basis $(u_1, \ldots, u_n)$ of V consisting of eigenvectors of f.

3.13 Some proofs

3.13.1 The Pythagorean theorem and reconstruction

Theorem 3.15. *Let V be a vector space over a field $\mathbb{F}$ and let $\langle,\rangle\colon V\times V\to\mathbb{F}$ be a bilinear form. Let $\|\ \|^2\colon V\to\mathbb{F}$ be the quadratic form associated to $\langle,\rangle$.*

(a) (Parallelogram property) If $x,y\in V$ then

$$\|x+y\|^2+\|x-y\|^2=2\|x\|^2+2\|y\|^2.$$

(b) (Pythagorean theorem) If $x,y\in V$ and $\langle x,y\rangle=0$ and $\langle y,x\rangle=0$ then

$$\|x\|^2+\|y\|^2=\|x+y\|^2.$$

(c) (Reconstruction) Assume that $\langle,\rangle$ is symmetric and that $2\neq 0$ in $\mathbb{F}$. Let $x,y\in V$. Then

$$\langle x,y\rangle=\tfrac{1}{2}(\|x+y\|^2-\|x\|^2-\|y\|^2).$$

Proof.
(a) Assume $x,y\in V$. Then

$$\begin{aligned}\|x+y\|^2+\|x-y\|^2&=\langle x+y,x+y\rangle+\langle x-y,x-y\rangle\\&=\langle x,x\rangle+\langle x,y\rangle+\langle y,x\rangle+\langle y,y\rangle+\langle x,x\rangle-\langle x,y\rangle-\langle y,x\rangle+\langle y,y\rangle\\&=2\|x\|^2+2\|y\|^2.\end{aligned}$$

(b) Assume $x,y\in V$ and $\langle x,y\rangle=0$ and $\langle y,x\rangle=0$. Then

$$\begin{aligned}\|x+y\|^2&=\langle x+y,+x+y\rangle=\langle x,x\rangle+\langle x,y\rangle+\langle y,x\rangle+\langle y,y\rangle\\&=\|x\|^2+0+0+\|y\|^2=\|x\|^2+0+0+\|y\|^2.\end{aligned}$$

(c) Assume $x,y\in V$. Then

$$\begin{aligned}\|x+y\|^2-\|x\|^2-\|y\|^2&=\langle x+y,x+y\rangle-\langle x,x\rangle-\langle y,y\rangle\\&=\langle x,x\rangle+\langle x,y\rangle+\langle y,x\rangle+\langle y,y\rangle-\langle x,x\rangle-\langle y,y\rangle\\&=2\langle x,y\rangle.\end{aligned}$$

□

3.13.2 Cauchy-Schwarz

Theorem 3.16. *Let $\mathbb{F}$ be a field with an involution $\bar{\ }\colon\mathbb{F}\to\mathbb{F}$ such that the fixed field*

$$\mathbb{K}=\{a\in\mathbb{F}\mid a=\bar{a}\}\qquad\textit{is an ordered field.}$$

For $a\in\mathbb{K}$ define

$$|a|^2=a\bar{a}.$$

Let V be an $\mathbb{K}$-vector space with a sesquilinear form $\langle,\rangle\colon V\times V\to\mathbb{F}$ such that

(a) If $x,y\in V$ then $\langle y,x\rangle=\overline{\langle x,y\rangle}$.

(b) If $x\in V$ then $\langle x,x\rangle\in\mathbb{K}_{\geq 0}$.

Let $\| \,\|\colon V \to \mathbb{F}$ be the corresponding quadratic form and assume that if $a \in \mathbb{K}_{\ge 0}$ then there exists a unique $c \in \mathbb{K}_{\ge 0}$ such that $c^2 = a$. Then

(c) (Cauchy-Schwarz) If $x, y \in V$ then $|\langle x, y\rangle| \le \|x\| \cdot \|y\|$.

(d) (Triangle inequality) If $x, y \in V$ then $\|x + y\| \le \|x\| + \|y\|$.

Proof. (c) Let $x, y \in V$. If $x = 0$ then both sides of the Cauchy-Schwarz inequality are 0. Assume $x \ne 0$. The Gram-Schmidt process on the vectors (x, y) suggests the consideration of

$$u_1 = \frac{x}{\|x\|} \qquad \text{and} \quad u_2 = y - \frac{\langle y, x\rangle}{\langle x, x\rangle} x.$$

To avoid denominators, let $u = \langle x, x\rangle y - \langle y, x\rangle x$. Then

$$\begin{aligned} 0 \le \langle u, u\rangle &= \big\langle \langle x, x\rangle y - \langle y, x\rangle x, \langle x, x\rangle y - \langle y, x\rangle x\big\rangle \\ &= \overline{\langle x, x\rangle}\langle x, x\rangle|\langle y, y\rangle - \langle x, x\rangle\overline{\langle y, x\rangle}\langle y, x\rangle - \langle y, x\rangle\overline{\langle x, x\rangle}\langle x, y\rangle + |\langle y, x\rangle|^2\langle x, x\rangle \\ &= \overline{\langle x, x\rangle}(\langle x, x\rangle\langle y, y\rangle - |\langle y, x\rangle|^2) \end{aligned}$$

Since $x \ne 0$ then $\langle x, x\rangle \in \mathbb{K}_{>0}$ and so $\overline{\langle x, x\rangle} = \langle x, x\rangle \in \mathbb{K}_{>0}$. Thus,

$$0 \le \langle x, x\rangle\langle y, y\rangle - |\langle y, x\rangle|^2 \qquad \text{and so} \qquad |\langle y, x\rangle|^2 \le \langle x, x\rangle\langle y, y\rangle.$$

Since the function $f\colon \mathbb{K}_{\ge 0} \to \mathbb{K}_{\ge 0}$ given by $f(z) = z^2$ is injective and monotone (Proposition 3.3) then $|\langle x, y\rangle| \le \|x\| \cdot \|y\|$.

(d) Let $a \in \mathbb{F}$. Using that if $z \in \mathbb{F}$ then $|z|^2 = z\bar{z} \in \mathbb{K}_{\ge 0}$, then

$$|a + \bar{a}|^2 \le |a + \bar{a}|^2 + |a - \bar{a}|^2 = (a + \bar{a})^2 - (a - \bar{a})^2 = 4a\bar{a} = 4|a|^2.$$

So $|a + \bar{a}| \le 2|a|$. Also

$$\text{if } a + \bar{a} \in \mathbb{K}_{\le 0} \text{ then } a + \bar{a} \le 0 \le |a + \bar{a}| \qquad \text{and} \qquad \text{if } a + \bar{a} \in \mathbb{K}_{\ge 0} \text{ then } a + \bar{a} = |a + \bar{a}|.$$

Combining these with $|a + \bar{a}| \le 2|a|$ gives

$$a + \bar{a} \le 2|a|.$$

Assume $x, y \in V$. Then

$$\begin{aligned} \|x + y\|^2 &= \langle x, x\rangle + \langle x, y\rangle + \langle y, x\rangle + \langle y, y\rangle \\ &= \|x\|^2 + |y\|^2 + \langle x, y\rangle + \overline{\langle x, y\rangle} \\ &\le \|x\|^2 + |y\|^2 + 2|\langle x, y\rangle| \\ &\le \|x\|^2 + |y\|^2 + 2\|x| \cdot \|y\| \\ &= (\|x\| + \|y\|)^2. \end{aligned}$$

Thus $\|x + y\| \le \|x\| + \|y\|$. $\square$

3.13.3 Nondegeneracy and dual bases

Proposition 3.17. *Let V be a vector space with a sesquilinear form $\langle,\rangle\colon V\times V\to\mathbb{F}$. Let $W\subseteq V$ be a subspace of V. Assume W is finite dimensional, that $(w_1,\ldots,w_k)$ is a basis of W and that G is the Gram matrix of $\langle,\rangle$ with respect to the basis $\{w_1,\ldots,w_k\}$. The following are equivalent:*

(a) A dual basis to $(w_1,\ldots,w_k)$ exists.

(b) G is invertible.

(c) $W\cap W^\perp=0$.

(d) The linear transformation

$$\begin{array}{cccc}\Psi_W\colon & W & \to & W^* \\ & v & \longmapsto & \varphi_v\end{array}\qquad \textit{given by}\qquad \varphi_v(w)=\langle v,w\rangle,$$

is an isomorphism.

Proof.
(a) $\Rightarrow$ (b): Assume that $\{w^1,\ldots,w^k\}$ exists.
To show: G is invertible.
Define $H(\ell,i)\in\mathbb{F}$ by

$$w^i=\sum_{\ell=1}^k H(i,\ell)w_\ell.$$

Then

$$\delta_{ij}=\langle w^i,w_j\rangle=\sum_{\ell=1}^k H(i,\ell)\langle w_\ell,w_j\rangle=\sum_{\ell=1}^k H(i,\ell)G(\ell,j)=(HG)(i,j).$$

So $HG=1$, H is the inverse of G, and G is invertible.
(b) $\Rightarrow$ (a): Assume that G is invertible.
For $i\in\{1,\ldots,k\}$ define

$$w^i=\sum_{\ell=1}^k G^{-1}(i,\ell)w_\ell,\qquad \text{for } i\in\{1,\ldots,k\}.$$

Then

$$\langle w^i,w_j\rangle=\sum_{\ell=1}^k G^{-1}(i,\ell)\langle w_\ell,w_j\rangle=\sum_{\ell=1}^k G^{-1}(i,\ell)G(\ell,j)=(G^{-1}G)(i,j)=\delta_{ij}.$$

So $\{w^1,\ldots,w^k\}$ is a dual basis to $\{w_1,\ldots,w_k\}$.
(b) $\Rightarrow$ (c): Assume that G is invertible.
To show: $W\cap W^\perp=0$.
Let $w\in W\cap W^\perp$.
To show: $w=0$.
Write $w=c_1w_1+\cdots+c_kw_k$.
To show: If $j\in\{1,\ldots,k\}$ then $c_j=0$.
Since $w\in W^\perp$ then $\langle w,w_r\rangle=0$ for $r\in\{1,\ldots,k\}$ and

$$\begin{aligned}c_j&=\sum_{\ell=1}^n c_\ell\delta_{\ell j}=\sum_{\ell=1}^n c_\ell G(\ell,r)G^{-1}(r,j)\\&=\sum_{\ell=1}^k c_\ell\langle w_\ell,w_r\rangle G^{-1}(r,j)=\sum_{r=1}^k\langle w,w_r\rangle G^{-1}(r,j)=0.=\sum_{r=1}^k 0\cdot G^{-1}(r,j)=0.\end{aligned}$$

So $w = 0$.
(c) $\Rightarrow$ (b): Assume that $W \cap W^\perp = 0$.
To show: G is invertible.
To show: The rows of G are linearly independent.
To show: If $c_1, \ldots, c_k \in \mathbb{F}$ and $(c_1, \ldots, c_k)G = 0$ then $c_1 = 0,\ c_2 = 0, \ldots,\ c_k = 0$.
Assume $c_1, \ldots, c_k \in \mathbb{F}$ and $(c_1, \ldots, c_k)G = 0$.
To show: $c_1 = 0,\ c_2 = 0, \ldots,\ c_k = 0$.
Let $w = c_1 w_1 + \cdots + c_k w_k$.
If $i \in \{1, \ldots, k\}$ then, since $(c_1, \ldots, c_k)G = 0$,

$$0 = \sum_{\ell=1}^{k} c_\ell G(\ell, i) = \sum_{\ell=1}^{k} c_k \langle w_\ell, w_i\rangle = \langle c_1 w_1 + \cdots c_k w_k, w_i\rangle = \langle w, w_i\rangle.$$

So $w \in W^\perp$.
So $w \in W \cap W^\perp$.
So $w = 0$.
So $c_1 = 0,\ c_2 = 0,\ \ldots, c_k = 0$.
Thus the rows of G are linearly independent and G is invertible.
(c) $\Rightarrow$ (d): Assume that $W \cap W^\perp = 0$
To show: $\Psi_W \colon W \to W^*$ is an isomorphism.
To show: (ca) Ψ_W is injective.
(cb) Ψ_W is surjective.

(ca) Since $\ker(\Psi_W) = W \cap W^\perp$ then $\ker(\Psi_W) = 0$.
So Ψ_W is injective.
(cb) If $\{w_1, \ldots, w_k\}$ is a basis of W then defining $\varphi^i \colon W \to \mathbb{F}$ by

$$\text{if } c_1, \ldots, c_k \in \mathbb{F} \text{ then} \qquad \varphi^i(c_1 w_1 + \cdots + c_k w_k) = c_i,$$

produces a basis $\{\varphi^1, \ldots, \varphi^k\}$ of the dual space W^*.
So $\dim(W) = \dim(W^*)$.
Since Ψ_W is injective W is finite dimensional then $\dim(\mathrm{im}(\Psi_W)) = \dim(W) = \dim(W^*)$.
So $\mathrm{im}(\Psi_W) = W^*$ and ψ_W is surjective.

So Ψ_W is an isomorphism.
(d) $\Rightarrow$ (c): Assume that Ψ_W is an isomorphism.
So Ψ_W is injective.
So $\ker(\Psi_W) = 0$.
Since $\ker(\Psi_W) = W \cap W^\perp$ then $W \cap W^\perp = 0$. □

3.13.4 Isotropy and nondegeneracy

Proposition 3.18. *A sesquilinear form $\langle , \rangle \colon V \times V \to \mathbb{F}$ satisfies*

(no isotropic vectors condition) If $v \in V$ and $\langle v, v\rangle = 0$ then $v = 0$.

if and only if it satisfies

(no isotropic subspaces condition) If W is a subspace of V then $W \cap W^\perp = 0$.

Proof. $\Rightarrow$: Assume that if $v \in V$ and $\langle v, v\rangle = 0$ then $v = 0$.
To show: If W is a subspace of V then $W \cap W^\perp = 0$.
Assume W is a subspace of V.
To show: If $w \in W \cap W^\perp$ then $w = 0$.
Assume $w \in W \cap W^\perp$.
Then $\langle w, w\rangle = 0$.
So $w = 0$.

$\Leftarrow$: Assume that if W is a subspace of V then $W \cap W^\perp = 0$.
To show: If $v \in V$ and $\langle v, v\rangle = 0$ then $v = 0$.
Assume $v \in V$.
To show: If $v \neq 0$ then $\langle v, v\rangle \neq 0$.
Assume $v \neq 0$.
Let $W = \mathbb{F}v$, a one-dimensional subspace of V.
Since $\mathbb{F}v \cap (\mathbb{F}v)^\perp = 0$ then $v \notin (\mathbb{F}v)^\perp$.
So $\langle v, v\rangle \neq 0$. □

3.13.5 Characterizing orthogonal projections

Proposition 3.19. *(Characterization of orthogonal projection) Let $\mathbb{F}$ be a field and let V be an $\mathbb{F}$-vector space. Let $\langle,\rangle\colon V \times V \to \mathbb{F}$ be a sesquilinear form. Let $k \in \mathbb{Z}_{>0}$ and let W be a subspace of V such that $\dim(W) = k$ and $W \cap W^\perp = 0$. The orthogonal projection onto W is the unique linear transformation $P\colon V \to V$ such that*

(1) If $v \in V$ then $P(v) \in W$.

(2) If $v \in V$ and $w \in W$ then $\langle v, w\rangle = \langle P(v), w\rangle$.

Proof. Let $(w_1, \ldots, w_k)$ be a basis of W and let $(w^1, \ldots, w^k)$ be the dual basis of W. The *orthogonal projection onto* W is the function

$$P_W\colon V \to V \qquad \text{given by} \qquad P_W(v) = \sum_{i=1}^{k} \langle v, w_i\rangle w^i.$$

To show: (a) P_W is a linear transformation that satisfies conditions (1) and (2).
(b) If Q is a linear transformation that satisfies (1) and (2) then $Q = P_W$.

(a) To show: (0) P_W is a linear transformation.
(1) If $v \in V$ then $P(v) \in W$.
(2) If $v \in V$ and $w \in W$ then $\langle v, w\rangle = \langle P(v), w\rangle$.

(0) To show: If $c \in \mathbb{F}$ and $v, v_1, v_2 \in V$ then $P_W(cv) = cP_W(v)$ and $P_W(v_1 + v_2) = P_W(v_1) + P_W(v_2)$.
Assume $c \in \mathbb{F}$ and $v, v_1, v_2 \in V$.
To show: $P_W(cv) = cP_W(v)$ and $P_W(v_1 + v_2) = P_W(v_1) + P_W(v_2)$.
Since $\langle,\rangle$ ls linear in the first coordinate then

$$P_W(cv) = \sum_{i=1}^{k} \langle cv, w_i\rangle w^i = \sum_{i=1}^{k} c\langle v, w_i\rangle w^i = c\Big(\sum_{i=1}^{k} \langle v, w_i\rangle w^i\Big) = cP_W(v), \quad \text{and}$$
$$P_W(cv) = \sum_{i=1}^{k} \langle v_1 + v_2, w_i\rangle w^i = \sum_{i=1}^{k} c\langle v_1, w_i\rangle w^i + \sum_{i=1}^{k} c\langle v_1, w_i\rangle w^i = PW(v_1) + P_W(v_2).$$

So P_W is a linear transformation.

(1) Assume $v \in V$.

Since $w^1, \ldots, w^k \in W$ and $P_W(v) = \sum_{i=1}^{k} \langle v, w_i \rangle w^i$ then $P_W(v) \in W$.

(2) Assume $v \in V$ and $w \in W$.

Since $\{w_1, \ldots, w_k\}$ is a basis of W then there exist $c_1, \ldots, c_k \in \mathbb{F}$ such that $w = c_1 w_1 + \cdots + c_k w_k$.

Then

$$\langle P_W(v), w \rangle = \Big\langle \sum_{i=1}^{k} \langle v, w_i \rangle w^i, \sum_{j=1}^{k} c_j w_j \Big\rangle = \sum_{i=1}^{k} \overline{c_i} \langle v, w_i \rangle = \langle v, w \rangle.$$

Thus $P_W(v)$ is a linear transformation that satisfies (1) and (2).

(b) Assume $Q\colon V \to V$ is a linear transformation that satisfies (1) and (2).
To show: $Q = P_W$.

To show: If $v \in V$ then $Q(v) = P_W(v)$.
Assume $v \in V$.
Since Q satisfies property (2), if $w \in W$ then $\langle Q(v), w \rangle = \langle v, w \rangle$.
So $\langle Q(v), w \rangle = \langle v, w \rangle = \langle P_W(v), w \rangle$.
So, if $w \in W$ then $\langle P_W(v) - Q(v), w \rangle = 0$.
So $P_W(v) - Q(v) \in W^\perp$.
By Property (1), $P_W(v) - Q(v) \in W$.
So $P_W(v) - Q(v) \in W \cap W^\perp$.
Since $W \cap W^\perp = 0$ then $P_W(v) - Q(v) = 0$.

So $P_W = Q$.

□

3.13.6 Orthogonal decomposition

Theorem 3.20. *Let $n \in \mathbb{Z}_{>0}$ and let V be an inner product space with $\dim(V) = n$. Let W be a subspace of V such that $W \cap W^\perp = 0$. Let P_W be the orthogonal projection onto W and let $P_{W^\perp} = 1 - P_W$. Then*

$$P_W^2 = P_W, \quad P_{W^\perp}^2 = P_{W^\perp}, \quad P_W P_{W^\perp} = P_{W^\perp} P_W = 0, \quad 1 = P_W + P_{W^\perp},$$

$$\ker(P_W) = W^\perp, \qquad \operatorname{im}(P_W) = W \quad \textit{and} \qquad V = W \oplus W^\perp.$$

Proof. (a) Assume $v \in V$. Then, by properties (1) and (2) of Proposition 3.7,

$$P_W^2(v) = \sum_{i=1}^{k} \langle P_W(v), w^i \rangle w_i = \sum_{i=1}^{k} \langle v, w^i \rangle w_i = P_W(v). \qquad \text{So } P_W^2 = P_W.$$

(b) Since $P_W^2 = P_W$ then

$$P_{W^\perp}^2 = (1 - P_W)^2 = 1 - 2P_W + P_W^2 = 1 - 2P_W + P_W = 1 - P_W = P_{W^\perp}.$$

(c) Since $P_W^2 = P_W$ and $P_{W^\perp} = 1 - P_W$ then

$$P_W P_{W^\perp} = P_W(1-P_W) = P_W - P_W^2 = P_W - P_W = 0 \quad \text{and}$$
$$P_{W^\perp} P_W = (1-P_W)P_W = P_W - P_W^2 = P_W - P_W = 0.$$

(d) Since $P_{W^\perp} = 1 - P_W$ then $P_W + P_{W^\perp} = P_W + (1-P_W) = 1$.

(e) To show $\ker(P_W) = W^\perp$.

To show: (ea) $\ker(P_W) \subseteq W^\perp$.

(eb) $W^\perp \subseteq \ker(P_W)$.

(ea) Assume $v \in \ker(P_W)$.
By property (2) in Proposition 3.7, $\langle v, w\rangle = \langle P_W(v), w\rangle = \langle 0, w\rangle = 0$.
So $v \in W^\perp$.
So $\ker(P_W) \subseteq W^\perp$.

(eb) Assume $v \in W^\perp$.
If $w \in W$ then $\langle P_W(v), w\rangle = \langle v, w\rangle = 0$ and so $P_W(v) \in W^\perp$.
By property (1), $P_W(v) \in W$ and so $P_W(v) \in W \cap W^\perp = 0$.
So $v \in \ker(P_W)$.
So $W^\perp \subseteq \ker(P_W)$.

So $\ker(P_W) = W^\perp$.

(f) To show: $\operatorname{im}(P_W) = W$.

To show: (fa) $\operatorname{im}(P_W) \subseteq W$.

(fb) $W \subseteq \operatorname{im}(P_W)$.

(fa) By property (1) of Proposition 3.7, $\operatorname{im}(P_W) \subseteq W$.

(fb) Assume $w \in W$.
Let $c_1, \ldots, c_k \in \mathbb{F}$ such that $w = c_1 w^1 + \cdots + c_k w^k$.
Since $\langle w^i, w_j\rangle = \delta_{ij}$ then

$$P_W(w) = \sum_{i=1}^k \langle w, w_i\rangle w^i = \sum_{i=1}^k \sum_{j=1}^k \langle c_j w^j, w_i\rangle w^i = \sum_{j=1}^k c_j w^i = w.$$

So $W \subseteq \operatorname{im}(P_W)$.

So $\operatorname{im}(P_W) = W$.

(g) If $v \in V$ then $v = P_W(v) + (1-P_W)(v) \in W + W^\perp$.
So $V = W + W^\perp$.
By assumption $W \cap W^\perp = 0$, and so $V = W \oplus W^\perp$.

□

3.13.7 Orthonormal sequences are linearly independent

Proposition 3.21. *Let V be an $\mathbb{F}$-vector space with a Hermitian form. An orthonormal sequence $(a_1, a_2, \ldots)$ in V is linearly independent.*

Proof. Let $(a_1, a_2, \dots)$ be an orthonormal sequence in V.
To show: $\{a_1, a_2, \dots\}$ is linearly independent.
To show: If $\ell \in \mathbb{Z}_{>0}$ and $\mu_1 a_1 + \mu_2 a_2 + \cdots + \mu_\ell a_\ell = 0$ then $\mu_j = 0$ for $j \in \{1, 2, \dots, \ell\}$.
Assume $\ell \in \mathbb{Z}_{>0}$ and $\mu_1 a_1 + \mu_2 a_2 + \cdots + \mu_\ell a_\ell = 0$.
To show: If $j \in \{1, \dots, \ell\}$ then $\mu_j = 0$.
Assume $j \in \{1, \dots, \ell\}$.
Then $0 = \langle \mu_1 a_1 + \mu_2 a_2 + \cdots + \mu_\ell a_\ell, a_j\rangle = \mu_j \langle a_j, a_j\rangle = \mu_j$.
So $\{a_1, a_2, \dots\}$ is linearly independent. □

3.13.8 Gram-Schmidt

Theorem 3.22. *(Gram-Schmidt) Let V be an $\mathbb{F}$-vector space with a sesquilinear form $\langle, \rangle \colon V \times V \to \mathbb{F}$. Assume that $\langle, \rangle$ is nonisotropic and that $\langle, \rangle$ is Hermitian i.e.,*

(1) (Nonisotropy condition) If $v \in V$ and $\langle v, v\rangle = 0$ then $v = 0$, and

(2) (Hermitian condition) If $v_1, v_2 \in V$ then $\langle v_2, v_1\rangle = \overline{\langle v_1, v_2\rangle}$.

Let $p_1, p_2, \dots$ be a sequence of linear independent elements of V.
(a) Define $b_1 = p_1$ and

$$b_{n+1} = p_{n+1} - \frac{\langle p_{n+1}, b_1\rangle}{\langle b_1, b_1\rangle} b_1 - \cdots - \frac{\langle p_{n+1}, b_n\rangle}{\langle b_n, b_n\rangle} b_n, \qquad \text{for } n \in \mathbb{Z}_{>0}.$$

Then $(b_1, b_2, \dots)$ is an orthogonal sequence in V.
(b) Assume that $\mathbb{F}$ is a field in which square roots can be made sense of and that if $v \in V$ and $v \neq 0$ then $\langle v, v\rangle \neq 0$. Define

$$\|v\| = \sqrt{\langle v, v\rangle}, \qquad \text{for } v \in V.$$

Let $(b_1, \dots, b_n)$ be an orthogonal basis of V. Define

$$u_1 = \frac{b_1}{\|b_1\|}, \quad \dots, \quad u_n = \frac{b_n}{\|b_n\|}.$$

Then $(u_1, \dots, u_n)$ is an orthonormal basis of V.

Proof. (Sketch) The proof is by induction on n.
For the base case, there is only one vector b_1 and so there is nothing to show.
Induction step: Assume $(b_1, \dots, b_n)$ are orthogonal.
Let $j \in \{1, \dots, n\}$. Then

$$\begin{aligned}
\langle b_{n+1}, b_j\rangle &= \left\langle p_{n+1} - \frac{\langle p_{n+1}, b_1\rangle}{\langle b_1, b_1\rangle} b_1 - \cdots - \frac{\langle p_{n+1}, b_n\rangle}{\langle b_n, b_n\rangle} b_n, b_j \right\rangle \\
&= \langle p_{n+1}, b_j\rangle - \frac{\langle p_{n+1}, b_1\rangle}{\langle b_1, b_1\rangle}\langle b_1, b_j\rangle - \cdots - \frac{\langle p_{n+1}, b_n\rangle}{\langle b_n, b_n\rangle}\langle b_n, b_j\rangle \\
&= \langle p_{n+1}, b_j\rangle - \frac{\langle p_{n+1}, b_j\rangle}{\langle b_j, b_j\rangle}\langle b_j, b_j\rangle = \langle p_{n+1}, b_j\rangle - \langle p_{n+1}, b_j\rangle = 0 \quad \text{and} \\
\langle b_j, b_{n+1}\rangle &= \left\langle b_j, p_{n+1} - \frac{\langle p_{n+1}, b_1\rangle}{\langle b_1, b_1\rangle} b_1 - \cdots - \frac{\langle p_{n+1}, b_n\rangle}{\langle b_n, b_n\rangle} b_n \right\rangle \\
&= \langle b_j, p_{n+1}\rangle - \frac{\overline{\langle p_{n+1}, b_1\rangle}}{\langle b_1, b_1\rangle}\langle b_j, b_1\rangle - \cdots - \frac{\overline{\langle p_{n+1}, b_n\rangle}}{\langle b_n, b_n\rangle}\langle b_j, b_n\rangle \\
&= \langle b_j, p_{n+1}\rangle - \frac{\overline{\langle p_{n+1}, b_j\rangle}}{\langle b_j, b_j\rangle}\langle b_j, b_j\rangle = \langle b_j, p_{n+1}\rangle - \overline{\langle p_{n+1}, b_j\rangle} = 0,
\end{aligned}$$

where the identity $\overline{\langle b_k, b_k\rangle} = \langle b_k, b_k\rangle$ and the last equality follow from the assumption that $\langle , \rangle$ is Hermitian. So $(b_1, \ldots, b_{n+1})$ are orthogonal. □

3.13.9 The role of normal matrices

Proposition 3.23. *Let $V = \mathbb{C}^n$ with inner product given by (3.1). Let*

$$A \in M_n(\mathbb{C}), \qquad \lambda \in \mathbb{C} \qquad \text{and} \qquad V_\lambda = \ker(\lambda - A).$$

If $AA^* = A^*A$ then

$$V_\lambda \text{ is } A\text{-invariant}, \quad V_\lambda^\perp \text{ is } A\text{-invariant}, \quad V_\lambda \text{ is } A^*\text{-invariant and} \quad V_\lambda^\perp \text{ is } A^*\text{-invariant.}$$

Proof.

(a) Let $p \in V_\lambda$. Then $Ap = \lambda p \in V_\lambda$. So V_λ is A invariant.
(b) Let $p \in V_\lambda$. Since $A(A^*p) = A^*Ap = \lambda A^*p$ then $A^*p \in V_\lambda$. So V_λ is A^* invariant.
(c) Let $z \in V_\lambda^\perp$.
To show $Az_\lambda \in V_\lambda^\perp$.
To show: If $u \in V_\lambda$ then $\langle Az, u\rangle = 0$.
Assume $u \in V_\lambda$.
To show: $\langle Az, u\rangle = 0$.
By (b), $A^*u \in V_\lambda$, and so $\langle Az, u\rangle = \langle z, A^*u\rangle = 0$.
So $Az \in V_\lambda^\perp$.
So $V_\lambda^\perp$ is A-invariant.
(d) Let $z \in V_\lambda^\perp$.
To show: If $u \in V_\lambda$ then $\langle A^*z, u\rangle = 0$.

$$\langle A^*z, u\rangle = \langle z, Au\rangle = 0, \qquad \text{since } Au \in V_\lambda.$$

So $A^*z \in V_\lambda^\perp$. So $V_\lambda^\perp$ is A^*-invariant.

□

3.13.10 The Spectral theorem

Theorem 3.24. *(Spectral theorem)*
Let $n \in \mathbb{Z}_{>0}$ and $V = \mathbb{C}^n$ with inner product given by (3.1).

(a) Let $n \in \mathbb{Z}_{>0}$ and $A \in M_n(\mathbb{C})$ such that $AA^* = A^*A$. Then there exists a unitary $U \in M_n(\mathbb{C})$ and $\lambda_1, \ldots, \lambda_n \in \mathbb{C}$ such that

$$U^{-1}AU = \mathrm{diag}(\lambda_1, \ldots, \lambda_n).$$

(b) Let $f\colon V \to V$ be a linear transformation such that $ff^* = f^*f$. Then there exists an orthonormal basis $(u_1, \ldots, u_n)$ of V consisting of eigenvectors of f.

Proof. The two statements are equivalent via the relation between A and f given by

$$\begin{array}{rccc} f\colon & V & \longrightarrow & V \\ & v & \longmapsto & Av. \end{array}$$

The proof is by induction on n.
The base case is when $\dim(V) = 1$. In this case $A \in M_1(\mathbb{C})$ is diagonal.
The induction step:
For $\mu \in \mathbb{C}$ let $V_\mu = \ker(\mu - f)$, the μ-eigenspace of f.
Since $\mathbb{C}$ is algebraically closed, there exists $\lambda \in \mathbb{C}$ which is a root of the characteristic polynomial $\det(x - A)$.
So there exists $\lambda \in \mathbb{C}$ such that $\det(\lambda - A) = 0$.
So there exists $\lambda \in \mathbb{C}$ such that $V_\lambda = \ker(\lambda - A) \neq 0$.
Let $k = \dim(V_\lambda)$ and let $(p_1, \ldots, p_k)$ be a basis of V_λ.
Use Gram-Schmidt to convert $(p_1, \ldots, p_k)$ to an orthogonal basis $(u_1, \ldots, u_k)$ of V_λ.
By definition of V_λ, the basis vectors $(u_1, \ldots, u_k)$ are all eigenvectors of f (of eigenvalue λ.
By Theorem 3.20 (orthogonal decomposition) and Proposition 3.12,

$$V = V_\lambda \oplus (V_\lambda)^\perp \quad \text{and } V_\lambda^\perp \text{ is } A\text{-invariant and } A^*\text{-invariant.}$$

Let

$$\begin{array}{rccc} f_1\colon & V_\lambda^\perp & \to & V_\lambda^\perp \\ & v & \mapsto & Av \end{array} \qquad \text{and} \qquad \begin{array}{rccc} g_1\colon & V_\lambda^\perp & \to & V_\lambda^\perp \\ & v & \mapsto & A^*v \end{array}$$

Then $g_1 = f_1^*$ and $f_1 f_1^* = f_1^* f_1$.
Thus, by induction, there exists an orthonormal basis $(u_{k+1}, \ldots, u_n)$ of $V_\lambda^\perp$ consisting of eigenvectors of f_1.
By definition of f_1, eigenvectors of f_1 are eigenvectors of f.
So $(u_1, \ldots, u_k, u_{k+1}, \ldots, u_n)$ is an orthonormal basis of eigenvectors of f. $\square$